Healthcare data breaches: Biometric technology to the rescue

Omotosho Folorunsho Segun[1], Fadiora Babatunde Olawale[2]

*[1,2] Computer Studies Department , Faculty of Science, The Polytechnic, Ibadan
Oyo State, Nigeria.*

Abstract - *Patient identification is the foundation of effective healthcare: the correct care needs to be delivered to the correct patient. However, relying on manual identification processes such as demographic searches and social security numbers often results in patient misidentification hence, the needs for electronic medical records (EMR). . It was discovered that many medical systems switching to electronic health records in order to explore the advantages of electronic medical records (EMR) creates new problems - by producing more targets for medical data to be hacked. Hackers are believed to have gained access to up to 80 million records that contained Social Security numbers, birthdays, postal addresses, and e-mail addresses.*

This work addresses this problem by exploring the security and privacy issues in healthcare sectors, and offers a comprehensive integration of biometrics technology applications in addressing the security challenges. Biometrics technology application in the health care industry refers to staff authentication and patient identification solutions. Usually, biometric is used to secure access to sensitive patient records and to assist with patient registration requirements. This includes biometric applications in doctors' offices, hospitals, monitoring patients, access control, workforce management or patient record storage.

The paper concludes that biometrics technology offers considerable opportunities to justify its application in Healthcare due to its ability to provide operational efficiencies that reduces costs, fraud, medical errors and increases patient satisfaction through reliable security solutions.

Key Words: Biometric, Identification, Authentication, Healthcare, Patients, Security.

1. INTRODUCTION

One of the primary concerns with maintaining data integrity is implementing a consistent approach across the healthcare industry. Information is needed to match patients with their data. Both physicians and patients have to trust and rely that their data is complete, current, accurate, and secure. With the healthcare industry optimism to rely on electronic health records, there is great concern about how digitizing health records will create massive efficiencies and significantly increase the quality of patient care [1]. As more and more hospitals and healthcare systems migrate to computerized physician order entry and electronic health records, and more health information exchanges are built to coordinate care across networks, many are raising concerns about how to effectively manage data integrity to ensure it is kept free from corruption, modification, or unauthorized access [3].

1.1 Electronic Medical Records

A medical record can span hundreds of pages consisting of text, graphs, and images. It contains information such as treatments received, medical history, life style details, family medical history, medications prescribed, and numerous other items pertinent to an individual's health. In the interests of the integrity of the health care industry and good patient care, it is recommended that these records should be retained for as long as possible. For these factors alone, it is obvious that the move toward electronic data capture will greatly assist in the storage and management of patient record [4] s. Although this change is long overdue, the healthcare industry has only recently begun to convert their paper records to electronic form using electronic medical record (EMR) systems [3, 4].

1.2 Description of Biometric Technology

Biometric identification technology provides automated methods to identify a person based on physical characteristics – such as fingerprints, hand shape, the eyes and face – as well as behavioral characteristics – including signatures and voice patterns as seen in figure 1. A biometric identification device is capable of measuring individual biometric information, comparing the resulting measurement with one or more stored biometric reference templates, deciding whether they match sufficiently to indicate that they represent the same person, and indicating whether or not a recognition or verification of identity has been achieved [10,11].

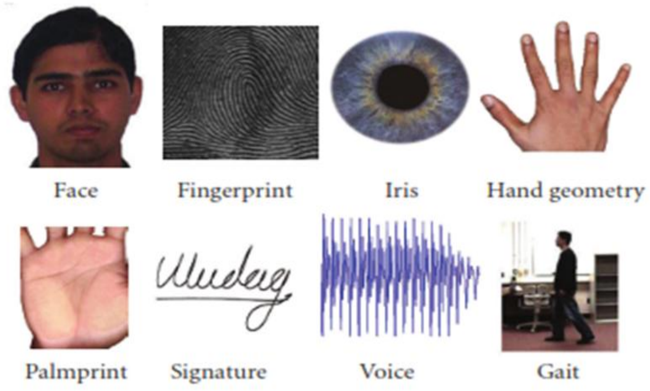


Figure1: Examples of body traits that can be used for biometric recognition. Anatomical traits include face, fingerprint, iris, palm print, hand geometry, and ear shape; while gait, signature, and keystroke dynamics are some of the behavioral characteristics. Voice can be considered as behavioral characteristic. (Adapted from Anil K Jain,)

It was discovered that many medical systems switching to electronic health records in order to explore the advantages of paperless exacerbates existing problems like duplicate and overlays. The mass rush to electronic medical records (EMR) creates new problems - by producing more targets for medical data to be hacked. Hackers are believed to have gained access to up to 80 million records that contained Social Security numbers, birthdays, postal addresses, and e-mail addresses [6,7].

This work addresses this problem by exploring the security and privacy issues in health care sectors, and offers a comprehensive integration of biometrics technology applications in addressing the security challenges.

Section II provides a critical analysis of related work while Section III gives detailed explanation of various biometric traits integration. Evaluation and ease of its use is discussed in Section IV with Section V concludes the paper by summarizing our contribution.

2. RELATEDWORK

The ultimate solution to maintaining end-to-end data integrity healthcare industries doesn't originate from one company but a collective and cost-effective effort from all healthcare providers across the industry.

With the healthcare industry aiming at total implementation of electronic health records, there is rampant optimism about how digitizing health records will not be breach. As more and more hospitals and healthcare systems migrate to computerized physician order entry and electronic health records, and more health information exchanges are built to coordinate care across networks, there is a great need to effectively manage data integrity to ensure it is kept free from corruption, modification, or unauthorized access [5].

Health information exchange data integrity and quality care originates with accurate patient identification [5]. There is simply no other step in patient care that is more important within the modern healthcare construct than precise patient identification to ensure that not only is the right care delivered to the right patient, but that medical records are up to date, accurate and properly linked across systems.

2.2 Biometric systems modes

Two different stages are involved in the biometric system process – enrollment and verification.

Enrollment: As shown in Figure 2A, the biometric sample of the individual is captured during the enrollment process (e.g., using a sensor for fingerprint, microphone for speech recognition, camera for face recognition, camera for iris recognition). The unique features are then extracted from the biometric sample (e.g., image) to create the user's biometric template [7]. This biometric template is stored in a database or on a machine-readable ID card for later use during a matching process.

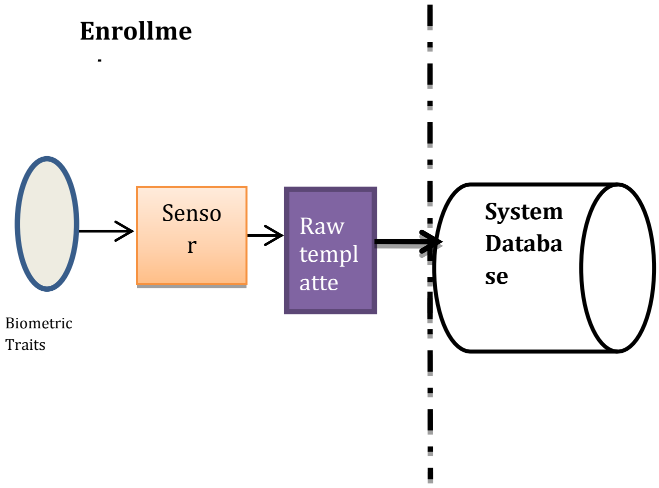


Figure 2A: A Generic Biometric System

Verification: Figure 2B illustrates the biometric verification process. The biometric sample is again captured. The unique features are extracted from the biometric sample to create the user's "live" biometric template. This new template is then compared with the template(s) previously stored in the system database and a numeric matching (similarity) score(s) is generated based on a determination of the common elements between the two templates. System designers determine the threshold value for this verification score based upon the security and convenience requirements of the system [6].

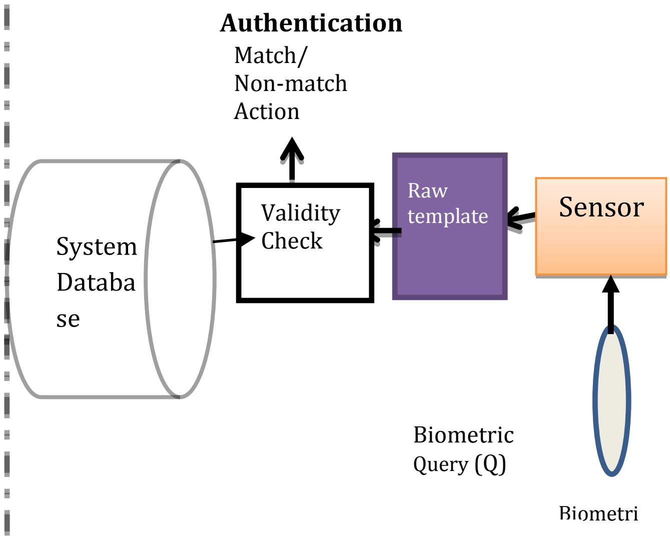


Figure 2B: A Generic Biometric System

2.3 Need for Biometrics in Healthcare

The need for biometrics in the healthcare industry is growing at astronomical rates; the worldwide market potential is currently estimated at $1.9 billion. A significant driver in biometric market growth rates is the HIPAA Act; HIPAA imposes stringent new federal requirements to protect patient privacy and the confidentiality of patient information. This is causing all healthcare facilities to begin developing compliance procedures for meeting these new standards. As a result, healthcare institutions are beginning to embrace the deployment of biometrics. Institutionalizing biometrics does indeed compliment the strategy in assuring HIPAA compliance through [3,4]

- User authentication
- Privacy of patient information
- Network security / PKI management
- Web security for e-business applications
- Internet authentication services
- Data storage and retrieval management

Biometrics also creates operational efficiencies for all identification procedures, it provides improvements to risk management programs by ensuring that accurate patient is tied into care or treatment plans or matched to medical records management systems for each individual patient. It also offers for the first time what many agencies have wanted – the concept of a universal patient identification number that provides positive identification of an individual using a biometric tied to a unique number [11]. And lastly, the overall quality of care is improved through accurate patient and/or staff identification.

Access Control

Biometrics plays an important role in healthcare applications, especially when there is a need to control access through positive identification of authorized users. HIPAA regulations mandate patient confidentiality and biometrics can help ensure that only authorized personnel gain access to those records. Biometrics help minimize insurance fraud and theft of controlled inventories such as pharmaceuticals and they can secure against the unauthorized use of expensive medical equipment [8]

Biometric identity solutions deter and reduce fraud by:

- improves patient care and protects patient privacy, [4]

- Preventing card sharing and patient identity theft by authenticating the patient in the provider's location.

- In fee-for-service programs, preventing provider billing for "phantom claims" or services when a patient is not at the provider location on the service date.

- Verifying managed care "encounter data" or services from providers so that Medicare and Medicaid programs can rely on this reported data for setting of managed care rates.

- Creating an "audit trail" of check in and check out times for comparison against type of service provided as an indicator of potential fraud called "upcoding."

3.0 Various biometric traits integration

The selection of the appropriate biometric traits will depend on a number application-specific factors, including the environment in which the identification or verification process is carried out, the user profile, requirements for matching accuracy and throughput, the overall system cost and capabilities, and cultural issues that could affect user acceptance. High, medium, and low are denoted by H, M, and L. Values assigned for how each biometric identifier meets the various qualities are subjective judgments, based on expert opinion (Smart Cards and Biometrics in Healthcare Identity Applications, [1,9]

Table -1: Comparison of Biometric Technologies Traits (Smart Cards and Biometrics in Healthcare Identity Applications, (2012)

Biometric Identifier	Maturity	Accuracy	Uniqueness	Failure-to-Enroll Rate	Record Size	Universality	Durability
Face	M	M	M	L	H 84-2,000	H	M
Fingerprint	H	H	M	L-M	M 250-1,000	M	M
Hand	M	L	L	L	L 9	M	M
Iris	M	M	H	L	M 688	M	H
Signature	L	L	M	L	M 500-1,000	M	M
Vascular	M	M	H	L	M 512	H	H
Voice	L	L	M	M	H 1,500-3,000	H	L

The factor in the selection of the appropriate biometric technology is its accuracy. When the live biometric template is compared to the stored biometric template in a verification application, a similarity score is used to confirm or deny the identity of the user. System designers set the threshold for this numeric score to accommodate the desired level of matching performance for the system, as measured by the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Biometric system administrators will tune sensitivity to FAR and FRR to get to the desired level of matching performance supporting the system security requirements [8].

- The False Acceptance Rate indicates the likelihood that a biometric system will wrongly accept an imposter.

- The False Rejection Rate indicates the likelihood that a biometric system will wrongly reject the correct person.

3.1 The Quality of Image Captured

In order for biometrics to provide positive outcomes, the accuracy or quality of fingerprint imaging is paramount. If images captured are not reliable, the risk of error due to improper or inaccurate identification increases dramatically [9].. Images In the healthcare industry requires the highest level of accuracy, which eliminates user error as well as increases acceptability of integration of biometric technology in healthcare industries.

3.2 The Usage

During enrollment: - The users have to physically scan his/her finger and the fingerprint sensor creates an image. The software will extract all the unique data points from that image and convert that into a biometric identity template. Iris recognition technology uses a very high-quality camera to extract the unique pattern present in your eye [8]. The results are mere binary strings—a series of zeroes and ones.

Verification: - When a patient returns, the company will take another scan of fingerprint or take another photograph with the iris camera depending on the biometric traits and perform what is called a one-to-many biometric search, in which the patient's iris scan is compared to the rest in the system.

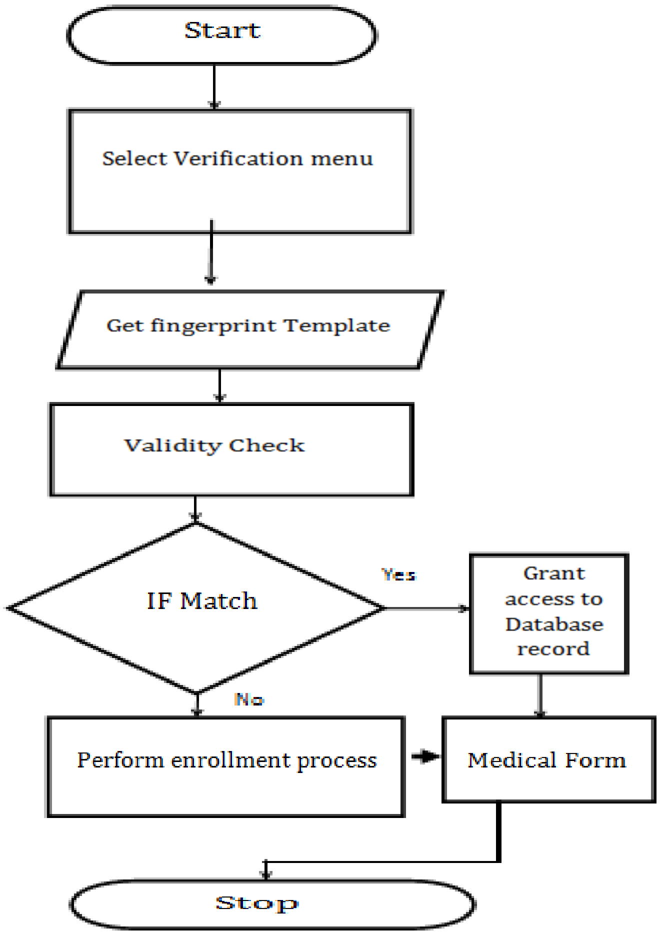


Figure 3: Program Flowchart

4.0 EVALUATION AND EASE OF USE

4.1 Database

The data used for the evaluation of the authentication system was gathered from 200 individuals. Collection of fingerprint images was carried-out through Fingerprint Live Scan Device (SecuGen 7.1).

4.2 Performance

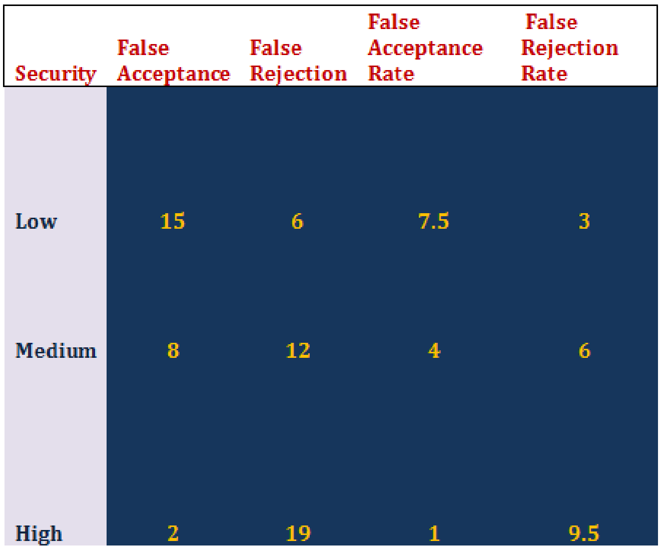
The model is capable of differentiating fingerprints at a good correct rate by setting an appropriate threshold value/Security level.

When total number of samples is two hundred (200)

Table 2: Evaluation indexes

False Acceptance Rate (FAR)	False Rejection Rate (FRR)
(%) FAR = (FA/N) * 100 FA = number of incidents of false acceptance N = total number of samples	(%) FRR = (FR/N) * 100 FR = number of incidents of false rejections. N = total number of samples.

Table 3: Incidences of False Acceptance and False rejection



Security	False Acceptance	False Rejection	False Acceptance Rate	False Rejection Rate
Low	15	6	7.5	3
Medium	8	12	4	6
High	2	19	1	9.5

It should be noted that there is a tradeoff between false acceptance rate and false rejection rate as shown in table 3.

4.3 Recommendation

As biometric patient identification systems continue to evolve, one can expect to see more modal biometric authentication solutions that combine multiple traits for patient identification such as fingerprint, iris and facial recognition. This provides healthcare with additional tools to accurately identify patients in the event of injury or trauma.

Some recommendations of using biometrics within healthcare include:

- Implement mobile biometric patient identification throughout a hospital to confirm the identity of patients at various touch points such as pre-op, medication dispensing and outpatient services.
- Increase ability to communicate with identifying an unconscious patient or those with the inability to speak or who may suffer from a language barrier.
- Increase data integrity standards across health information exchanges (HIEs).
- Implement biometric automated systems to decrease the potential for inaccurate patient identification.
- Implement Voice Authentication – The client's voice is their password, there is no need to remember passwords, PINs, policy numbers or other challenge information.
- Implement Voice Signature – Secure, legally binding signature over the phone using client's voice print.

5. CONCLUSIONS

All over the world, governments, corporations, military establishments and others are using biometric technology for identification objectives. The use of biometrics is rapidly becoming the de-facto means of person authentication in healthcare because there is no other method more safe, secure, affordable, or efficient.

Patient safety continues to be one of healthcare's most pressing challenges, although there are many angles from which patient safety can be addressed, the prevention of duplicate medical records and the elimination of medical identity theft stand out as two of the main culprits jeopardizing the integrity of the healthcare industry. in addition placing patient safety at risk, the root cause of these problems are generally inaccurate patient identification, a problem that can be rectified through the adoption of biometric technology.

REFERENCES

[1] A Strong Pulse for Biometrics in Healthcare. (2013, September 27) From http://www.planetbiometrics.com/article-details/i/1745/

[2] Biometric Identity in Healthcare: Reduces Health Care Fraud, Improves Patient Care and Protects Patient Privacy. (2011, July) From http://www.ibia.org/download/datasets/727/

[3] Healthcare Biometric Identity Management Technology. from http://www.versos.com.sa/solutions/iss/iam/healthcare_biometric_iam.htm

[4] Schneider, John K. (2011). Positive Outcomes Implementing Biometrics in Multiple Healthcare Applicationshttp://www.ultrascan.com/Portals/16/PositiveOutcomes.pdf

[5] Spence, B. (2011, November 4). Hospitals can finally put a finger on biometrics. from http://www.securityinfowatch.com/article/10473265/hospitals-can-finally-put-a-finger-on-biometrics

[6] Trader, John. (2012, September 26). Why Healthcare Should Evaluate Biometrics for Patient Identification. from http://www.porterresearch.com/Resource_Center/Blog_News/Blog/2012/September/

[7] J. George Annas. The Rights of Patients. Southern Illinois University Press, Car- bondale, Illinois, 2004.

[8] D'Arcy Guerin Gue. The HIPAA Security Rule (NPRM): http://www.hipaadvisory.com/regs/securityoverview.htm.

[9] HHS. Protecting the Privacy of Patients' Health Information. http://www.hhs.gov/news/facts/privacy.html.

[10] A. K. Jain, A. Ross, and S. Pankanti, (2006), "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143,

[11] S. Krawczyk, S., & A Jain (2005). Securing electronic medical records using biometric authentication. In Audio-and Video-Based Biometric Person Authentication (pp. 435-444). Springer Berlin/Heidelberg.

[12] M. Gudavalli., D. S. Kumar & S.V. Raju (2014). Integrated Biometric Template Security using Random Rectangular Hashing. Global Journal of Computer Science and Technology, 14(7).